REMARKS

Claims 15-24 and 27-34 are pending in the present application, claims 25-26 and 35 having been cancelled without prejudice or disclaimer herein. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

Claims 15-24 and 27-34 were rejected under 35 U.S.C. §112, second paragraph. Applicants have amended the claims to overcome this rejection. Applicants have attempted, and believe that they have, addressed each of the noted concerns by rewriting claims to positively recite the method steps and clarify the claimed invention. Withdrawal of this rejection is respectfully requested.

Claims 15-24 and 27-34 were rejected under 35 U.S.C. §103 as being unpatentable over Applicants' admitted prior art in view of Chow (U.S. Patent No. 6,594,761) and Kocher (U.S. Patent No. 6,278,783). These rejections are respectfully traversed for the following reasons.

Claim 34 recites a method of executing and validating a cryptographic protocol between a server entity and a microcircuit card in order to resist a DPA attack against the microcircuit card during execution of said cryptographic protocol. The method comprises the steps of storing a first chain of operations in both the server entity and the microcircuit card, the first chain of operations forming a data encryption standard, storing, at the microcircuit card, a second chain of operations based on the first chain of operations stored in said microcircuit card, the second chain of operations comprising a succession of operations each corresponding to a complement of one of the operations in the first chain of operations, sending a message from the server entity to the microcircuit card, executing, at the server entity, the first chain of operations stored therein using the message to obtain a

server result, identifying, in the microcircuit card, a selected chain of operations, the step of identifying comprising randomly choosing one of the following groups as the selected chain: 1) all of the operations in the first chain of operations; 2) all of the operations in the chain of operations; or 3) a plurality of operations comprising a random selection of at least one of the operations in the first chain of operations and at least one of the operations in the second chain of operations, executing, in the microcircuit card, the identified chain of operations on the message, outputting a result of a last operation executed in the identified chain of operations either in an uncomplemented state or a complemented state as a resultant message, comparing the resultant message to the server result, and validating the cryptographic protocol between the server entity and the microcircuit card when the server result and the resultant message are identical. This is not taught, disclosed or made obvious by the prior art of record.

The Office Action acknowledges that the Applicants' admitted prior art does not disclose determining the second chain of operations as derived from the first chain, or that the determination is made by randomly selecting to perform operations of the first chain in either a normal or a complemented states. As claim 34 now recites, Applicants' admitted prior art does not disclose randomly selecting to perform as the selected chain: operations from the first or second chain, *i.e.*, 1) all of the operations in the first chain of operations; 2) all of the operations in the chain of operations; or 3) a plurality of operations comprising a random selection of at least one of the operations in the first chain of operations and at least one of the operations in the second chain of operations. The Office cites Chow and Kocher as allegedly disclosing these features. Applicants respectfully disagree.

First, Chow relates to tamper resistant software encoding, *i.e.,* he discloses a method and system for making computer software resistant to tampering and reverse-engineering. Thus, his method is useful for hiding the encryption and decryption routines. Chow helps to protect against changing the computer software in a manner that is against the original author's wishes (*see* col. 1, lines 57-67). It is a method and system that can be used when the user has access to the software code and can thus modify it. However, Applicants' method relates to a system in which the program is not accessible from outside of the microcircuit entity, and therefore cannot be modified. This is reflected in amended claim 34 in that the claim refers to a microcircuit card. In microcircuit cards, such as smartcards, the construction is such that the execution code for running the computing processor of the card is not accessible and not modifiable from outside. Moreover, Chow does not relate to a method or system of authenticating a server entity and a microcircuit card; it relates only to a method whereby tampering with user-accessible source code is made tamper-resistant. One of ordinary skill in the art faced with the problems associated with Applicants' admitted prior art would not have been motivated to look to patents in the art of tamper-resistant software to find solutions to those problems. Therefore, one of ordinary skill in the art would not have found it obvious to combine the teachings of Chow with the features of Applicants' admitted prior art.

The Office Action cites to col. 18, line 50-col. 19, line 13, of Chow as allegedly teaching "determining whether to perform an operation or its complement." However, as now clarified, Applicants' invention is different than the method disclosed in Chow. In the cited portion of Chow, Chow teaches a method of using a bit-exploded coding technique to encode one virtual register or other variable into multiple VRs or other variables. According to the patented technique, for bit-wise Boolean operations, either the operation or

its complement on each bit is performed. Col. 18, lines 65-66. However, the patent does not teach the claimed invention of, *inter alia*, identifying, in the microcircuit card, a selected chain of operations, the step of identifying comprising randomly choosing one of the following groups as the selected chain: 1) all of the operations in the first chain of operations; 2) all of the operations in the chain of operations; or 3) a plurality of operations comprising a random selection of at least one of the operations in the first chain of operations and at least one of the operations in the second chain of operations, executing, in the microcircuit card, the identified chain of operations on the message, and outputting a result of a last operation executed in the identified chain of operations either in an uncomplemented state or a complemented state as a resultant message. As these steps are not taught or used in Applicants' admitted prior art or in Chow, the resulting combination, even if assumed to have been obvious (an assumption with which Applicants disagree), would not yield the claimed invention recited in claim 34.

The Office Action cites Kocher as allegedly disclosing "a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13)." Applicants respectfully disagree.

Kocher discloses using additional random state information in the cryptographic processing. The random state information is mixed with the keys, plaintext messages, and intermediate quantities used during processing (this is stated in the cited portion of Kocher). The specifics of how the random state information is used in the patent is disclosed in column 6, lines 39-63. Col. 2, lines 17-18 disclose mixing random state information in with the keys. It does not disclose randomly choosing to decide which group

of a plurality of groups of instructions to execute, as recited in claim 1. Thus, since Kocher does not disclose using a random number generation for deciding which of a plurality of groups, or chains, of operations to execute, the proposed combination, even if assumed to have been obvious (an assumption with which Applicants disagree), would not yield the claimed invention recited in claim 34.

Further, Applicants respectfully submit that none of the references disclose or suggest "outputting a result of a last operation executed in said identified chain of operations either in an uncomplemented state or a complemented state as a resultant message" as recited in claim 34.

For at least these reasons, Applicant respectfully submits that claim 34 is patentable over the prior art of record whether taken alone or in combination as proposed in the Office Action.

Claim 22 depends from claim 34, and recites that the step of randomly choosing comprises generating a random parameter that is used to identify which of said groups to choose, and wherein said method further comprises updating a complementation counter at each generation of the random parameter, and the step of outputting as the resultant message is decided depending on a state of the complementation counter to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message. Claim 23 depends from claim 34, and recites that the step of randomly choosing comprises generating a random parameter that is used to identify which of said groups to choose, and wherein said method further comprises transmitting, with each executed operation, information to be used during the step of outputting the resultant message to determine whether to output the result of the last

operation in the uncomplemented state or the complemented state as the resultant message. Claim 31 depends from claim 34, and recites that the step of randomly selecting at least one of the operations in the first chain of operations and at least one of the operations in the second chain of operations comprises generating a random parameter before each operation is selected and updating a complementation counter, and the step of outputting as the resultant message is decided depending of a state of the complementation counter to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message. Claim 32 depends from claim 34, wherein the step of randomly selecting at least one of the operations in the first chain of operations and at least one of the operations in the second chain of operations comprises generating a random parameter before each operation is selected and wherein said method further comprises transmitting, with each executed operation, information to be used during the step of outputting the resultant message to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message.

None of these claimed steps are taught, disclosed or made obvious by the prior art of record, whether taken alone or in combination as proposed in the Office Action. The Office Action cites column 9, lines 7-13, 30-48 and 62-64 of Kocher as allegedly teaching the steps of claims 22 and 23 and 31 and 32, and particularly that "new operations are determined based on a random parameter". However, Applicants submit that this is different than the claimed method steps, which comprise generating a random parameter that is used to identify which of the listed groups of operations to choose for identification (claims 22 and 23) or generating a random parameter before each operation is selected (claims 31 and 32).

The Office Action cites column 9, lines 25-27 as allegedly teaching the claimed counter recited in claims 22 and 31. Applicants respectfully disagree. The Kocher counter is a failure counter – it is incremented at the beginning of the key and message update process. Kocher does not disclose incrementing a counter when a random parameter before each operation is selected (claim 31), or at each generation of the random parameter (claim 22).

Further, Applicants submit that none of the cited references discloses transmitting, with each executed operation, information to be used during the step of outputting the resultant message to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message, as recited in claims 23 and 32. The Office Action cites column 2, lines 17-19 of Kocher as allegedly disclosing this feature. However, this section states "[t]he random state information is mixed with the keys, plaintext messages, and intermediate quantities used during processing." Nothing in that portion of Kocher, or in any other, discloses transmitting, with each executed operation, information to be used during the step of outputting the resultant message to determine whether to output the result of the last operation in the uncomplemented state or the complemented state as the resultant message.

For at least these reasons, Applicants respectfully submit that claims 22, 23, 31 and 32 are patentable in and of themselves and as they depend from claim 34, which is patentable for the reasons discussed above. Additionally, Applicants respectfully submit that claims 15-19, 24-30, and 33 are patentable in and of themselves and as they depend from claim 34, which is patentable for the reasons discussed above.

In view of the above amendment and remarks, Applicant respectfully requests reconsideration and withdrawal of the outstanding rejections of record. Applicant submits that the application is in condition for allowance and early notice to this effect is most earnestly solicited.

If the Examiner has any questions he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:ma
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
\\bnsbs\vol1\BN\R\RINU\Akkar1\pto\2009-02-19-Amendment.doc